

DESCRIPTION

SYSTEM AND METHOD FOR REFLECTING PERSONAL INFORMATION ON  
INFORMATION PROCESSING TERMINAL BY CARRYING THE PERSONAL  
INFORMATION

5

TECHNICAL FIELD

The present invention relates to a system for using  
portable hardware having a rewritable data recording area  
to carry around personal data for connecting to a network  
and to reflect the personal data on an arbitrary  
10 information processing terminal, and in accordance  
therewith, enabling the use on an arbitrary information  
processing terminal of network services aimed at a  
specific individual.

BACKGROUND ART

15

Recently, personal computers and other information  
processing terminals have come into widespread use in  
ordinary homes, and users of networks, such as the  
Internet, are steadily increasing year by year. Further,  
electronic mail, news groups and other exchanges of  
20 information are being actively carried out in line with  
the increase of Internet users.

And, for a network-based exchange of information, so  
long as there is an environment that enables  
instantaneous, low-cost connection to a network thereof,  
25 the convenience of being able to send and receive  
information even when one is not at home, such as at the

workplace, at school, in a public facility, on the street, and so forth, is treasured.

However, as is often the case, an OS (operating system) and communications software of an information processing terminal must carry out numerous settings for connecting to a network in order to send and receive information using a network. If a user does not carry his or her personal data for connecting to the Internet (e.g. a password, IP (Internet protocol) address, and so forth assigned by a connection vendor) around at all times, the user still encounters inconveniences, such as not being able to connect to the Internet from a computer at one's destination for exchanging electronic mails.

#### DISCLOSURE OF THE INVENTION

It is a convenient method with outstanding instantaneity, costs, and portability to use a network typified by the Internet for sending and receiving information (hereinafter, the word "network" will signify all aspects for connecting computers to enable them to communicate with one another, without distinguishing between the Internet and an intranet). However, in order to connect to a network, it is necessary to input a user's personal data into each information processing terminal being used.

When carrying out this work, a certain degree of knowledge related to computers and networks is required,

and this work is extremely time consuming. Hence, even if having an information processing terminal at hand, it is difficult to make immediate use of a network at the time one wants to use it.

5 Further, vital personal data for connecting to a network is recorded in the information processing terminal that is used. Hence, there is a danger of misuse of this data, and from the standpoint of security, it is desirable to delete this data.

10 However, the deleting of the above-mentioned data is also difficult and time-consuming work, and this is an impediment to using a network safely.

Therefore, an object of the present invention is to enable data for connecting to a network to be easily  
15 carried around.

Another object of the present invention is to enable the above-mentioned data to be readily reflected in an information processing terminal.

Yet another object of the present invention is to  
20 enable the reflected data to be easily deleted when information processing terminal utilization has ended.

And yet another object of the present invention is to enable the above-mentioned data to be reflected in an information processing terminal, without being recorded  
25 inside the information processing terminal.

A system according to a first aspect of the present invention comprises an information processing terminal, and a portable-type personal data recording device which can be connected to the information processing terminal.

5 The personal data of a specific user is recorded in the personal data recording device. The information processing terminal has a personal data acquiring component for acquiring the personal data from the personal data recording device when the personal data

10 recording device is connected to the information processing terminal, and a personal data reflecting component for reflecting the acquired personal data in the information processing terminal and for setting the information processing terminal in a state desired by the

15 specific user.

With this system, by connecting a personal data recording device, which a specific user carries around with him or her, to an arbitrary information processing terminal, the personal data of the specific user, which

20 is recorded in the personal data recording device, is read into the information processing terminal, and reflected in the information processing terminal. As a result thereof, the specific user is able to set an arbitrary information processing apparatus to a desired

25 state.

In a preferred embodiment, there is disposed in the information processing terminal an preset information clearing component which, when the above information processing terminal has preset personal data, clears the preset personal data prior to reflecting the personal data from the above-mentioned personal data recording device, and a restoring component which, after personal data from the above-mentioned personal data recording device has been reflected, deletes the personal data from the information processing terminal and once again reflects in the information processing terminal the above-mentioned preset personal data, which had been clear beforehand. In accordance therewith, in addition to preset personal data being safeguarded, the security of personal data inside the above-mentioned personal data recording device is ensured.

A portable-type personal data recording device according to a second aspect of the present invention can be carried by a specific user, can be connected to an information processing terminal, has a user data recording area readable from the information processing terminal, and records in the user data recording area the specific user's personal data for setting the information processing terminal to a desired state of the specific user.

An information processing terminal according to a third aspect of the present invention can be connected to a portable-type personal data recording device that records the personal data of a specific user, and  
5 comprises a personal data acquiring component for acquiring personal data from the personal data recording device when connected to the personal data recording device, and a personal data reflecting component for reflecting the acquired personal data in the information  
10 processing terminal, and setting the information processing terminal to a desired state of the specific user.

A computer program product according to a fourth aspect of the present invention has a computer program  
15 for making a computer function as the above-mentioned information processing terminal.

A network utilization system according to a fifth aspect of the present invention comprises an information processing terminal having a network utilization function  
20 component, and a portable-type personal data recording device which can be connected to the information processing terminal. The personal data of a specific user is recorded in the portable-type personal data recording device. This personal data is information  
25 required for connecting to a network such that the specific user can utilize the above-mentioned information

processing terminal, and for receiving network services directed at a specific user. And the above-mentioned information processing terminal has a personal data acquiring component for acquiring the above-mentioned personal data from the personal data recording device when the personal data recording device is connected to the information processing terminal, and a private data reflecting component for reflecting in the information processing terminal the above-mentioned personal data acquired by the personal data acquiring component so that the network utilization function component is set in a state where the function is able to connect to the network such that the specific user can utilize the network and utilizes network services.

With this system, by connecting a personal data recording device, which a specific user carries with him or her, to an arbitrary information processing terminal having a network connection function, the personal data of the specific user, which is recorded in the personal data recording device, is read into the information processing terminal, and reflected in the information processing terminal. As a result thereof, it is possible for the specific user to use an arbitrary information processing terminal, connect to a network such that he is able to utilize the network (for example, connect to the Internet using his own Internet connection account), and

receive network services directed to himself (for example, send and receive electronic mail by using his own electronic mail account).

In a preferred embodiment, the above-mentioned  
5 personal data comprises network connection information required for connecting to a network such that the specific user can utilize the network, and personal communications information required for receiving network services directed at the specific user. Further, if the  
10 specific user so desires, personal environment information for customizing the environment inside an information processing terminal to suit the specific user can also be included in the above-mentioned personal data.

In a preferred embodiment, there is disposed in an  
15 information processing terminal an preset information clearing component which, when the above-mentioned information processing terminal has preset personal data, clears the preset personal data prior to reflecting the personal data from the above-mentioned personal data  
20 recording device, and a restoring component which, after the personal data from the above-mentioned personal data recording device has been reflected and network utilization in accordance with the personal data is over, deletes the personal data from the information processing  
25 terminal and once again reflects in the information processing terminal the above-mentioned preset personal



data, which had been clear beforehand. In accordance therewith, in addition to preset personal data being safeguarded, the security of personal data inside the above-mentioned personal data recording device is ensured.

5           A network utilization method according to a sixth aspect of the present invention has a step for preparing a portable-type personal data recording device that records personal data for connecting to the above-mentioned network, a step for connecting the data  
10 recording device to an information processing terminal having a network utilization function component, a step for reading the personal data recorded in the data recording device into the information processing terminal, and a step for reflecting the read personal data in the  
15 information processing terminal.

          A personal data recording device according to a seventh aspect of the present invention can be carried around by a specific user, can connect to an information processing terminal, and has a user data recording area  
20 that is readable from the information processing terminal. And personal data for connecting to the network is recorded in the user data recording area.

          An information processing terminal comprising a network utilization function component according to an  
25 eighth aspect of the present invention can connect to the above-mentioned portable-type personal data recording

device, and comprises a personal data acquiring component for acquiring personal data from the personal data recording device, and a personal data reflecting component for reflecting the acquired personal data in the information processing terminal. By connecting to the personal data recording device, which a specific user carries around, the information processing terminal can be readily set to a state in which the information processing terminal can connect to the network such that the specific user can utilize the network to receive network services directed to the specific user.

A computer program product according to a ninth aspect of the present invention has a computer program for making a computer having a network utilization function component functions as an information processing terminal according to the above-mentioned eighth aspect of the invention.

A data input device according to a tenth aspect of the present invention can be connected to a portable-type personal data recording device having a user data recording area, and comprises a personal data inputting component for inputting the personal data of a specific user for connecting the network, and a personal data transmitting component for transmitting the inputted personal data to the personal data recording device, and for recording the personal data in the user data

recording area in the the personal data recording device.  
With this data input device, personal data of a user can  
be recorded in a portable-type personal data recording  
device.

5           A computer program product according to an eleventh  
aspect of the present invention has a computer program  
for making a computer function as a data input device  
according to the above-mentioned tenth aspect.

#### BRIEF DESCRIPTION OF THE DRAWINGS

10           Fig. 1 is a block diagram showing a constitution of  
portable-type hardware (interkey), which is used in a  
network utilization system related to an embodiment of  
the present invention, and which records personal data  
for connecting to a network;

15           Fig. 2 is a block diagram showing a constitution of  
interkey-recorded personal data for connecting to a  
network;

            Fig. 3 is a block diagram showing an example of a  
hardware constitution of an information processing  
20   terminal, and an overall constitution of a network  
utilization system related to an embodiment of the  
present invention;

            Fig. 4 is a block diagram showing an example of a  
software constitution of an information processing  
25   terminal;

Fig. 5 is a flowchart showing a processing flow of the information processing terminal 21 when the interkey 1 is connected to the information processing terminal 21 and used therewith;

5 Fig. 6 is a continuation of the flowchart of Fig. 5;

Fig. 7 is a continuation of the flowchart of Fig. 6;

Fig. 8 is a diagram showing an example of a user interface screen of the information processing terminal 21 when the interkey 1 owner check is performed;

10 Fig. 9 is a diagram showing an example of a user interface screen of the information processing terminal 21 when preset personal data existing inside the information processing terminal 21 is being cleared;

Fig. 10 is a diagram showing an example of a user interface screen of the information processing terminal 15 21 when personal data 11 from the interkey 1 is being read in;

Fig. 11 is a diagram showing an example of a user interface screen of the information processing terminal 20 21 when connecting to a server on a network using personal data 11 from the interkey 1;

Fig. 12 is a diagram showing an example of a user interface screen of the information processing terminal 21 when deleting personal data 11 from the interkey 1;

25 Fig. 13 is a diagram showing an example of a user interface screen of the information processing terminal

21 when restoring the personal data setting of the information processing terminal 21 to the original setting;

Fig. 14 is a block diagram showing a software constitution of a data input terminal 51 for recording personal data 11 in the interkey 1;

Fig. 15 is a flowchart showing a processing flow of interkey read-write software 53 of the data input terminal 51 when recording the personal data 11 in the interkey 1;

Fig. 16 is a continuation of the flowchart of Fig. 15;

Fig. 17 is a continuation of the flowchart of Fig. 16;

Fig. 18 is a diagram showing an example of a user interface screen of the data input terminal 51 when inputting network connection information into the data input terminal 51;

Fig. 19 is a diagram showing an example of a user interface screen of the data input terminal 51 when inputting personal communications information into the data input terminal 51;

Fig. 20 is a diagram showing an example of a user interface screen of the data input terminal 51 when selecting a desired item from among personal environment information; and

Fig. 21 is a diagram showing an example of a user interface screen of the data input terminal 51 displaying a list of personal data that has been either inputted or selected.

5                    BEST MODE FOR CARRYING OUT THE INVENTION

Fig. 1 shows a constitution of portable-type hardware, which records personal data for connecting to a network, and which is used with a network utilization system related to an embodiment of the present invention.

10            As for this network utilization system, an individual user carries around hardware 1 like that shown in Fig. 1, which records personal data for connecting to a network. In the explanation hereinbelow, this portable-type hardware 1 is called an "interkey."

15            The interkey 1 comprises a user data **memory** area 3, which uses, for example, **RAM** for recording the personal data of a user for connecting to a network; a firmware recording area 5, which uses, for example, **ROM**, which is programmed firmware for processing the inputting and  
20    outputting of the personal data; an input-output (I/O) controller 7 for exchanging personal data between the user data **memory** area 3 and the below-described information processing terminal by executing the firmware; and an input-output terminal 9 (I/O port, for  
25    example, a **USB** device port) for physically connecting the

I/O controller 7 to the below-described information processing terminal.

As shown in Fig. 2, the above-mentioned user personal data 11 for connecting to a network is recorded  
5 in the user data **memory** area 3 of an interkey 1. And the personal data 11 comprises network connection information 13, and personal communications information 15. Further, if a user so desires, personal environment information 17 can also be included in the personal data 11. Here,  
10 network connection information 13 is personal data required for connecting to a network. Personal communications information 15 is personal data required for logging in to a server that provides a specific service after connecting to a network. Further, personal  
15 environment information 17 is personal data showing user customized settings for hardware and software within an information processing terminal. The specific contents of these data 13 to 17 will be explained hereinafter. Furthermore, a user-specific personal code (not shown in  
20 figure) for use when checking whether or not a user is the rightful owner of the interkey 1 is also recorded in the user data **memory** area 3.

As shown in Fig. 3, an interkey 1 is used by connecting it to an arbitrary information processing  
25 terminal 21 (for example, a personal computer, personal digital assistant (PDA), or hand-held telephone, that is,

a terminal comprising hardware and software, which is capable of connecting to a network). As will be explained in detail hereinbelow, an information processing terminal 21 reads the personal data 11 for  
5 connecting to an network that is recorded in the interkey 1, the personal data 11 is reflected in the information processing terminal 21, and in accordance therewith, an interkey 1 user can use the information processing terminal 21, connect to a network, and utilize a desired  
10 service. The information processing terminal 21 can be constituted such that the personal data 11 is automatically deleted from the information processing terminal 21 after use, or the personal data 11 is not recorded inside the information processing terminal 21  
15 during use, and in accordance therewith, the security of the personal data 11 is ensured.

With regard to the shape of an interkey 1, and the method for connecting an interkey 1 to an information processing terminal 21, anything will do so long as it is  
20 capable of executing operations in accordance with the principle of the present invention. A number of examples will be shown hereinbelow.

#### 1. Examples of shape of interkey 1

- (1) Hardware with built-in semiconductor memory.
- 25 (2) Card having either a magnetic or an optical recording media, such as a cash card.



(3) Card with a built-in IC, such as an IC card.

(4) Transmitter that emits radio waves of a specific wavelength.

2. Examples of methods for connecting an interkey 1  
5 to an information processing terminal 21

(1) Connect to the communications port (input-output  
port) 23 of an information processing terminal 21 (Refer  
to Fig. 3).

(2) Pass a recording magnetic body through hardware that  
10 reads the information of a magnetic or optical recording  
medium.

(3) Insert an IC card into hardware that reads IC  
information.

(4) Receive a radio wave with hardware capable of  
15 receiving a radio wave of a specific wavelength.

The specific contents of the network connection  
information 13, personal communications information 15,  
and personal environment information 17 contained in the  
personal data 11 shown in Fig. 2 will differ slightly  
20 depending on the software and hardware that is used, but  
the following contents can be given as examples.

1. Network connection information 13

(1) Access point to be connected (telephone number)

A telephone number of a place at which an  
25 information processing terminal (2) will access a network.

(2) Access username

Name for accessing a network.

(3) Access password

Password for accessing a network.

(4) TCP/IP setting

5        Settings of communications equipment, and accessed  
server, which are connected to an information processing  
terminal (2).

2. Personal communications information 15

(1) Mail sender's name

10        Name on an electronic mail message, and a name that  
is generally recognized as a mail sender.

(2) Mail address

Electronic mail address.

(3) Mail username

15        Name for accessing a mail server.

(4) Mail password

Password for accessing a mail server.

(5) Receiving mail server settings

Type and domain name of receiving mail server.

20        (6) Sending mail server settings

Type and domain name of sending mail server.

(7) Proxy server settings

Confirmation of proxy server use, and address, port  
number, and so forth.

25        (8) Need for password authentication

Confirmation of use of security-protected password authentication.

### 3. Personal environment information 17

#### (1) Browser customization information

5 Individual setting (options, security, and so forth) information of a browser.

#### (2) Mail software customization information

Individual setting (options, and so forth) information of mail software.

#### 10 (3) Selection of FEP type

Standard information on front end processor to be started.

#### (4) OS customization information

Setting information of OS, which uses browser, and  
15 mail software.

Any information processing device can be used as an information processing terminal 21 to which an interkey 1 is connected, so long as it has a basic environment for being connected to a network, and a function necessary  
20 for reading personal data from an interkey 1. Here, a basic environment for connecting to a network indicates an environment, which meets the conditions necessary for making a hardware connection to a network, and the above-mentioned personal data 11, and settings thereof are not  
25 included in the above-mentioned basic environment in the initial state. As examples of information processing

terminals 21 it is possible to cite a personal computer, PDA, hand-held telephone, game computer, home electrical appliance having a network connection function, and car navigation system. Examples of typical hardware and software constitutions of an information processing terminal 21 are shown in Fig. 3 and Fig. 4.

As shown in Fig. 3, an information processing terminal 21 comprises hardware, such as an I/O port (for example, a USB host port) 23, to which an interkey 1 can be connected, memory 25, firmware ROM 27, a CPU 31, and various other devices (including network connection hardware). As shown in Fig. 4, an information processing terminal 21 comprises software, such as an OS 47, network connection software 45, electronic mail software 41, and an Internet web browser 43.

To constitute an interkey 1 such that it can be utilized by the information processing terminal 21, either hardware or a software module, having functions for accessing an interkey 1, reading in personal data 11 from the interkey 1, and reflecting the personal data 11 in the information processing terminal 21, is incorporated into the appropriate hardware or software inside the information processing terminal 21, or new hardware or software having functions such as these is added to the information processing terminal 21. As one example thereof, in this embodiment, a software module

(hereinafter referred to as an interkey utility) 42, having functions for using an interkey 1, is added to electronic mail software 41. By virtue of the interkey utility 42 carrying out processing such that personal data 11 is read in from an interkey 1, and reflected in electronic mail software 41, an Internet browser 43, and network connection software 45 inside an information processing terminal 21, the new functions enumerated hereinbelow are substantially added on to the conventional functions shown hereinbelow in the electronic mail software 41, Internet browser 43, and network connection software 45.

#### 1. Electronic mail software 41

##### (1) Newly-added functions

- a) Function for clearing preset data on electronic mail software 41.
- b) Function for customizing electronic mail software 41 for user use according to personal environment information 17.
- c) Function for connecting to a mail server in accordance with personal communications information 15.
- d) Function for transferring a username and password in accordance with personal communications information 15.
- e) Function for deleting all temporary data for temporary work such as receiving mail, and sending mail.

f) Function for restoring cleared information and environment information to electronic mail software 41.

(2) Conventional functions

a) Function for registering/modifying/deleting a setting  
5 at the discretion of a user.

b) Function for connecting to a mail server via a user-selected setting.

c) Function for confirming a username and password.

d) Mail creating function.

10 e) Mail receiving function.

f) Mail sending function.

g) Function for separating and storing as files on arbitrary media received mail, and sent mail.

h) Function for closing electronic mail software 41.

15 2. Internet browser 43

(1) Newly-added functions

a) Function for clearing preset data on browser 43.

b) Function for customizing for a user security and functions in accordance with personal environment

20 information 17.

c) Function for deleting all temporary data, such as new temporary files, and a history list.

d) Function for restoring cleared data and environment information to the browser 43.

25 (2) Conventional functions

a) Function for customizing security and function settings, and plug-in-based functions at a user's discretion.

b) Function for moving to a website.

5 c) Function for various processing on the browser 43.

d) Function for closing the browser 43.

### 3. Network connection software 45

#### (1) Newly-added functions

a) Function for performing a dial-up connection according  
10 to network connection information 13 obtained from an interkey 1.

b) Function for disconnecting a dial-up connection in accordance with network connection information 13.

c) Function for deleting obtained network connection  
15 information 13.

#### (2) Conventional functions

a) Function for registering/modifying/deleting a connection setting at a user's discretion.

b) Function for performing a dial-up connection via a  
20 user-selected setting.

c) Function for disconnecting a dial-up connection in accordance with a user-selected setting.

The operation of this embodiment under the above constitution will be explained hereinbelow.

25 Fig. 5 to Fig. 7 show a processing flow of an information processing terminal 21 when making use of an

interkey 1 by connecting it to the information processing terminal 21. Fig. 8 to Fig. 13 show graphic user interface screens displayed on the information processing terminal 21 display at this time.

5           A user carries around an interkey 1 in which his personal data 11 has been recorded beforehand. As a method for recording personal data 11 in an interkey 1, an interkey 1 can be equipped with a data input function, such as a key input device, or a pen input device, and  
10          personal data can be inputted, and recorded in the interkey 1 only, or an interkey 1 can be connected to a device having a data input function, such as, for example, a personal computer, PDA, or hand-held telephone, and personal data can be recorded in the interkey 1 by using  
15          the hardware and software of this data input device (In the case of the latter, the processing flow for recording personal data will be explained hereinbelow by referring to Fig. 15-Fig. 21.).

          Next, a user connects an interkey 1 to an arbitrary  
20          information processing terminal 21 in which his personal data is not recorded (Fig. 5, Step S1). At this point, as explained hereinabove, a basic environment for connecting to a network must be prepared beforehand in the information processing terminal 21.

25          The information processing terminal 21 accesses the connected interkey 1, and the user's personal data 11



recorded in the interkey 1 is read into the information processing terminal 21, and is reflected in either the hardware or software inside the information processing terminal 21 via the procedures hereinbelow (Fig. 5, S2 and thereafter). This processing, as explained hereinabove, can be performed by either appropriate hardware or software inside an information processing terminal 21 having functions for using an interkey 1, and in this embodiment, as one example, this processing is carried out based around an interkey utility 42 added in to the electronic mail software 41 shown in Fig. 4. This processing will be explained in order hereinbelow.

Firstly, electronic mail software 41 is started by a user, upon which the interkey utility 42 added thereto accesses the interkey 1 connected to an I/O port 23, and recognizes same (Fig. 5, S2). Next, in a case in which the interkey utility 42 is set beforehand such that it performs an interkey 1 owner check (checks to determine whether or not the user is the rightful owner of the interkey 1) (Fig. 5, Yes at S3), an owner check is executed (Fig. 5, S4). In this owner check, the interkey utility 42 displays a screen such as that shown in Fig. 8, prompts the user to input a personal code, checks the inputted personal code against the personal code recorded in the interkey 1, and if they are identical, makes a determination that the user is the rightful owner (Fig. 5,

No at S5), and if they are not identical (Fig. 5, Yes at S5), determines that the user is not the rightful owner, and ends processing for using the interkey 1 (Fig. 5, S6).

If there is no problem with the owner check (or, if  
5 the setting is such that an owner check is not performed), the interkey utility 42 checks whether or not personal data for connecting to a network is preset inside the information processing terminal 21 prior to reading in personal data 11 from the interkey 1 (Fig. 5, S7), and in  
10 a case in which there are the preset personal data, it makes a determination by querying the user as to whether or not the preset personal data will be safeguarded (Fig. 5, S8). As a result thereof, if the preset personal data is to be safeguarded (Fig. 5, Yes at S8), a screen such  
15 as that shown in Fig. 9 is displayed, the user is prompted to confirm, and when the user clicks on OK on the screen, the preset personal data is stored in a prescribed storage area (either memory or storage) of the information processing terminal 21, and cleared (Fig. 5,  
20 S9). Conversely, if it is not necessary to safeguard the preset personal data (Fig. 5, No at S8), the preset personal data is destroyed (Fig. 5, S10).

Next, the interkey utility 42 queries the user as to whether or not the personal environment information 17 of  
25 the interkey 1 is to be used (Fig. 6, S11), and if the user responds that the personal environment information

17 of the interkey 1 is to be used (Fig. 6, Yes at S11),  
personal environment information 17 is read in from the  
interkey 1, and is reflected in the settings of either  
the electronic mail software 41, Internet browser 43,  
5 network connection software 45, or OS 47 of the  
information processing terminal 21 (Fig. 6, S12).  
Further, the interkey utility 42 checks whether or not  
the information processing terminal 21 is currently  
connected to a network (Fig. 6, S13), and in a case in  
10 which there is a connection, checks whether or not the  
user can utilize the current connection (Fig. 6, S14),  
and in a case in which the user can utilize the current  
connection, queries the user as to whether or not he will  
utilize the current connection as-is (Fig. 6, S15). As a  
15 result thereof, in a case in which the user responds that  
he will utilize the current connection (Fig. 6, Yes at  
S15), the current connection is maintained as-is, and  
processing moves to Step S21 of Fig. 7. On the other  
hand, in a case in which the user cannot utilize the  
20 current connection (Fig. 6, No at S14), or in a case in  
which the user responds he will not utilize the current  
connection even though he is capable of using same (Fig.  
6, No at S15), the interkey utility 42 uses the network  
connection software 45 to end the current connection (Fig.  
25 6, S16).

In a case in which a current connection is disconnected as described hereinabove (Fig. 6, S16), or in a case in which the information processing terminal 21 was not connected to a network (Fig. 6, No at S13), next, 5 the interkey utility 42 checks whether or not user-usable network connection information already exists in the information processing terminal 21 (Fig. 6, S17), and if there is preset user-usable network connection information (Fig. 6, Yes at S17), the interkey utility 42 10 queries the user as to whether or not he will make use thereof (Fig. 6, S18). As a result thereof, in a case in which either user-usable network connection information does not exist in the information processing terminal 21 (Fig. 6, No at S17), or, even though there is preset 15 network connection information, the user responded that he will not make use of same (Fig. 6, No at S18), the interkey utility 42 reads in network connection information 15 from the interkey 1, and reflects same in the network connection software 45 of the information 20 processing terminal 21 (Fig. 6, S19). Next, the interkey utility 42 starts the network connection software 45, and connects to a network using either network connection information 13 from the interkey 1, or preset network connection information, which the user responded he would 25 use (S20). By doing as explained hereinabove, a user-usable network connection is established (For example,

the user logs in to a DNS server of an Internet provider with whom he has a contract, and a connection is established to the Internet.). Thereafter, the interkey utility 42 moves to Step S21 of Fig. 7, reads in personal communications information 13 from the interkey 1, and reflects same in the settings of either electronic mail software 41 or an Internet browser 43 of the information processing terminal 21 (Fig. 7, S21). By doing as explained hereinabove, while personal data 11 is being read in from the interkey 1, and reflected in the information processing terminal 21, the interkey utility 42 displays a screen such as that shown in Fig. 10.

Thereafter, either the electronic mail software 41 or the Internet browser 43 connects to an electronic mail server or a Web server using the personal communications information 15 from the interkey 1 set in Step S21 of Fig. 7, and sends and receives contents, such as electronic mail or an HTML file (Fig. 7, S22). When a connection is being made to either an electronic mail server or a Web server, the interkey utility 42 displays a screen such as that shown in Fig. 11, informing the user that a connection is being made with information from the interkey 1. By so doing, the user can utilize his own dedicated network service using his own personal data.

When the network utilization ends (Fig. 7, S23), the interkey utility 42 queries the user as to whether or not

to restore the personal data settings of the information terminal 21 (Fig. 7, S24). If the user responds that the personal data settings will not be restored (Fig. 7, No at S24), the interkey utility 42 ends processing in a state wherein the personal data 11 from the interkey 1, which was reflected in the information processing terminal 21, is left inside the information processing terminal 21 as-is (S28). Conversely, if the user responds that the personal data settings are to be restored (Fig. 7, Yes at S24), the interkey utility 42 checks whether or not the preset personal data is being stored (Fig. 7, S25), and if not being stored (Fig. 7, No at S25), destroys the personal data 11 from the interkey 1, which had been reflected in the information processing terminal 21 (Fig. 7, S26), and thereafter, ends processing (S28). Conversely, if preset personal data is being stored (Fig. 7, Yes at S25), after destroying the personal data 11 from the interkey 1, which had been reflected in the information processing terminal 21, the interkey utility 42 reflects the stored preset personal data in its original state in the information processing terminal 21 (Fig. 7, S27), and thereafter, ends processing (S28). At this time, the interkey utility 42, while destroying the personal data 11 from the interkey 1, displays a screen such as that shown in Fig. 12, and, while restoring the stored preset personal data to its

original state, displays a screen such as that shown in Fig. 13.

By changing each of the settings of an information processing terminal 21 in accordance with personal environment information 17 from the interkey 1, it becomes possible for a user to connect to a network using an arbitrary information processing terminal 21 under the same conditions as the environment which the user ordinarily uses on his own terminal. Further, using an arbitrary information processing terminal 21, it is possible to connect to a network using network connection information 13 from an interkey 1, and following network connection, to receive services from various servers using personal communications information 15 from an interkey 1.

Further, among the personal data 11 for connecting to a network, depending on the time and circumstances, there is information, like network connection information 13, which either need not be reflected on an information processing terminal 21 or cannot be reflected thereon. For example, as explained hereinabove, in a case in which an information processing terminal 21 already has user-usable network connection information, or in a case in which an information processing terminal 21 is already connected to a network, and the user is permitted to utilize the network connection, it is possible to use a

network access environment that exists inside an information processing terminal 21 as-is without using the network connection information 13 inside an interkey 1.

5        Furthermore, in a case in which an information processing terminal 21 uses an OS 47 which cannot utilize personal data inside an interkey 1, it is also possible to constitute the present invention such that OS-dependent items among the information inside an interkey 10 1 are not automatically reflected. In this case, it is also possible to prepare an artificial OS environment in accordance with either software or hardware processing.

      Further, when an attempt is made to reflect personal data 11 inside an interkey 1 in an information processing terminal 21, in cases in which another person's personal data is already set in the information processing terminal 21, or the personal information of the previous user of the information processing terminal 21 remains, the preset personal data can be temporarily cleared and 20 safeguarded in a storage area. Then, after a network connection is completed via personal data 11 from an interkey 1, and recording of required information is over, the personal data 11 from an interkey 1 is deleted from the information processing terminal 21, and the preset 25 personal data, which was cleared, can be reset, and the information processing terminal 21 restored to its



original state. Or, at the discretion of the user, it is also possible not to delete personal data 11 from an interkey 1, and in accordance therewith, in a case in which a user possesses a plurality of information processing terminals 21, the work of setting personal data 11 in these plurality of information processing terminals 21 for connecting to a network can be done easily.

Furthermore, in the operations indicated in Fig. 5 to Fig. 7, personal data 11 from an interkey 1 is recorded one time in an information processing terminal 21, but as another method, it is also possible not to record personal data 11 from an interkey 1 in an information processing terminal 21. By not recording personal data 11 from an interkey 1 in an information processing terminal 21, it is possible to construct a system with higher security, and in addition, can lead to reduced time and labor by doing away with the need for an operation for deleting the personal data 11 from an information processing terminal 21 when network utilization has ended.

Furthermore, either the hardware or the software inside an information processing terminal 21 for using an interkey 1 can either be initially incorporated in an information processing terminal 21, or can be incorporated at a later time. Software for using an

interkey 1 can either be a component that is incorporated into another software like the interkey utility 42 shown in Fig. 4, or can be a dedicated software that is independent from other software.

5 By carrying around the above-mentioned interkey 1, individual users can readily carry personal data 11 for connecting to a network without carrying around an information processing terminal 21, and a user can easily set a variety of information processing terminals 21 to a  
10 usable state. Consequently, even at a business trip destination or travel destination, a user can utilize a network by operating an arbitrary information processing terminal by the same accustomed procedures as when ordinarily using his own information processing terminal.  
15 In accordance therewith, it is possible to carry out convenient, speedy information communications, and it is possible to utilize a network more effectively than in the past.

Next, a constitution and operation for recording  
20 personal data 11 in an interkey 1 will be explained. Here, there will be explained a case in which an interkey 1 is connected to a terminal device having a data inputting function, such as, for example, a personal computer, PDA, or hand-held telephone, and personal data  
25 11 is recorded in an interkey 1 using the hardware and software of the data input terminal.

Fig. 14 shows a software constitution of a data input terminal 51 for recording personal data 11 in an interkey 1. As shown in the figure, the data input terminal 51 has an OS 55, and interkey read-write software for recording personal data in an interkey 1. The hardware constitution of the data input terminal 51, for example, can be the same as that of the information processing terminal 21 shown in Fig. 3. Further, in the case of most users, since a user will probably use his own information processing terminal 21, which he ordinarily uses, as a data input terminal 51, information processing terminal 21 software, such as the electronic mail software 41, Internet browser 43, and network connection software 45 shown in Fig. 3, is also loaded in the data input terminal 51, and accordingly, oftentimes the personal data of the user already exists in the data input terminal 51. If interkey read-write software 53 is utilized, as is clear from the operation explanation hereinbelow, user personal data, which already exists in a data input terminal 51, can be easily transferred to an interkey 1.

Fig. 15 to Fig. 17 show an interkey read-write software 53 processing flow of a data input terminal 51 when recording personal data 11 in an interkey 1. Fig. 18-Fig. 21 show examples of user interface screens of the

interkey read-write software 53, which are displayed on a data input terminal 51 display at that time.

A user connects an interkey 1 to a data input terminal 51 (Fig. 15, S31), and starts the interkey read-write software 53. The interkey read-write software 53 recognizes the interkey 1, and searches for personal data 11 inside the interkey 1 (Fig. 15, S32). If there is personal data 11 inside the interkey 1 (Fig. 15, Yes at S33), the interkey read-write software 53 queries the user as to whether or not to delete the personal data 11 inside the interkey 1 (Fig. 15, S34), and if the user responds not to delete, personal data recording processing is ended (Fig. 15, S36), but if the user responds to delete, the personal data 11 inside the interkey 1 is deleted (or, a user data storage area 3 inside the interkey 1, which was shown in Fig. 2, is formatted) (Fig. 15, S35).

In the above-mentioned Step S35, after deleting the personal data 11 inside the interkey 1, or in a case in which there was no preset personal data 11 inside the interkey 1 (Fig. 15, No at S33), the interkey read-write software 53 prompts the user to input two times a personal code for use in an owner check (Fig. 15, S37, S38), and if the twice inputted personal code is the same (Fig. 15, Yes at S39), this personal code is transmitted

to the interkey 1, and stored inside the user data memory area 3 (Fig. 16, S40).

Next, the interkey read-write software 53 searches for preset network connection information and preset  
5 personal communications information inside the data input terminal 51 (Fig. 16, S41), and if there is either preset network connection information or preset personal communications information (Fig. 16, Yes at S42), the interkey read-write software 53 queries the user as to  
10 whether or not the preset information will be used in the interkey 1 (Fig. 16, S43), and if the user responds that it will be used, the preset information is automatically entered onto an input screen on the interkey read-write software 53 (Fig. 16, S44), and then processing jumps to  
15 Step S49 of Fig. 17.

Conversely, in a case in which there is no preset network connection information or preset personal communications information inside the data input terminal 51 (Fig. 16, No at S42), or, in a case in which the user  
20 responds that neither preset network connection information nor preset personal communications information will be automatically transmitted (Fig. 16, No at S43), the interkey read-write software 53 displays a screen like that shown in Fig. 18, and prompts the user  
25 to input network connection information on to the screen (Fig. 16, S45). Thereafter, when the user makes an input

to the effect that the inputted network connection information is correct (for example, when he clicks the "Next" button of the screen of Fig. 18) (Fig. 16, Yes at S46), the interkey read-write software 53 subsequently displays a screen like that shown in Fig. 19, and prompts the user to input personal communications information on to the screen (Fig. 16, S47). Thereafter, when the user makes an input to the effect that the inputted personal communications information is correct (for example, when he clicks the "Next" button of the screen of Fig. 19) (Fig. 16, Yes at S48), the interkey read-write software 53 subsequently progresses to Step S49 of Fig. 17.

In Step S49 of Fig. 17, the interkey read-write software 53 searches for preset personal environment information inside the data input terminal 51. As a result thereof, if there is preset personal environment information inside the data input terminal 51 (Fig. 17, Yes at S50), the interkey read-write software 53 displays a screen like that shown in Fig. 20, and prompts the user to select which items within the personal environment information will be transmitted to the interkey 1 (Fig. 17, S51). When the user selects an item, and makes an input to the effect that this is correct (for example, when he clicks the "Next" button of the screen of Fig. 20) (Fig. 17, Yes at S52), the interkey read-write software 53 subsequently displays a screen like that

shown in Fig. 21, and lists on the screen the network connection information, personal communications information, and personal environment information, which the user either inputted or selected in Steps S45-S51 up  
5 until this time (Fig. 17, S53).

Thereafter, when the user makes an input to the effect that all the inputted information, which is listed, is correct (for example, when he clicks on the "Finish" button of the screen of Fig. 21) (Fig. 17, Yes at S54),  
10 the interkey read-write software 53 transmits all of the inputted information to the interkey 1, stores it inside the user data **memory** area 3 (Fig. 17, S55), and then ends the processing of this data recording (Fig. 17, S56). The personal data, which the user either inputted or  
15 selected, is hereby recorded in the interkey 1.

Although, hereinabove, explanateion has been made with referece to one embodiment of the present invention, this embodiment is strictly an example for explaining the present invention, and does not purport to limit the  
20 present invention to the above embodiment alone.

Therefore, the present invention can also be implemented in a variety of aspects other than the above embodiment without deviating from the gist thereof.